WHITEPAPER

Gaia-X secure and trustworthy ecosystems with Self Sovereign Identity

Developing a Decentralised, User-Centric, and Secure Cloud Ecosystem

Abstract

This white paper explains the key concerns, architecture and principles of Self-Sovereign Identity (SSI) as it applies in the Gaia-X ecosystem. Self-Sovereign Identity ensures secure and trustworthy digitalisation in the decentralised ecosystem that Gaia-X aims to be. Without the need for a conventional central Identity Management System (IdM), the Self-Sovereign Identity concept enables any subject, such as a person, organisation or even a machine, to manage their digital identities and associated credentials like membership cards, certificates or Self-Descriptions in a self-sovereign manner. Crypto standards and Self-Sovereign Identity standards, in combination with Web3-compliant technology components, enable the Gaia-X ecosystem to gain the required level of trust without the need for centrally hosted and controlled Identity Providers (IDPs).

Table of Contents

Why build a cloud ecosystem with SSI?

Given the high economic potential of the next generation Web3 in line with data protection requirements, many businesses and governments have recognised the importance of Self-Sovereign Identity (SSI) and have already started the adoption of SSI on a global scale. Covid tracker and test and vaccination certificate apps, in particular, have accelerated its adoption. The European Union is investing heavily in the Decentralised Identity Framework ESSIF (European Self Sovereign Identity Framework) used for next-generation digitalisation (Web3) in the public and private sector.

However, the SSI ecosystem will only be accepted and adopted by users if it provides unique data protection benefits and the technologies used are future-proof. Another important factor for establishing trust in the next-generation digital world is the appropriate community support following open-source principles, standards, and wide adoption in popular software components around Cloud Native Compute Foundation (CNCF)[2].

Business and social relevance of an SSI ecosystem for digital identities

The following subitems highlight aspects of an SSI and cloud ecosystem that are relevant for the economy and society:

Digitalisation and acceptance by citizens

Digitalisation is of high business relevance, as the use of innovative technologies helps to simplify processes and make them more efficient. It is, therefore, a vital factor in maintaining competitiveness. Many users would like processes and procedures to be simplified using digital technologies. However, there is also a lack of trust in how user data is collected, handled, and processed. Using the current pattern, by requiring the user to accept comprehensive terms and conditions before accessing a service, the user does not know exactly what they are giving permission for.

Despite the scepticism, users want companies to build up and regain trust[3]. They expect companies to act responsibly and trustworthy when providing new technologies: only when users believe that their trust is justified will they accept and use new technologies and information technology (IT) services. The Self-Sovereign Identity (SSI) approach can help build this trust because it is designed to be user-centric and user-experience-friendly with fine granular control of permissions and data usage.

The economic relevance of an SSI ecosystem for digital identities

Manually executed processes and media breaks[1] are the reason for inefficient processes and thus impair optimal productivity. The economic and political relevance of accelerated digitalisation can be derived from this. Use cases show, for example, how the optimisation of supply chains can be implemented by means of digitalisation, which enables digital and well-structured verifiable credentials to be processed easily, quickly, securely and in a trustworthy manner. The implementation of digital identities and credentials has an exceptionally high economic benefit for application development companies.

The SSI approach both offers a high degree of sovereignty and has enormous economic potential.

---

1) In information processing, a media break occurs when the content received via an information medium is transferred to another in the transmission chain of the process and must be recreated again.
2) https://www.cncf.io/
3) https://www.dotmagazine.online/issues/building-trust/trustworthiness-creates-trust

Technological sovereignty

Technological sovereignty is an increasingly important factor since – in the short to medium term – the added value share of information technology and the Internet, and thus the data in all industries, will increase enormously. For free, independent, and comprehensive use, in terms of shaping our society, the development of competencies and key technologies must be promoted in a targeted manner in critical key sectors. This is the only way of counteracting potential risks that may arise because of dependencies on the market leaders. In addition, an early positioning in innovative technologies and concepts is of decisive relevance in remaining competitive in the global, national or European arena. This requires reducing dependencies, confidently and trustworthily designing the use of future relevant technologies, and also actively promoting them. SSI technology is crucial for digital identities and enables greater autonomy to be achieved with regard to the use and exploitation of personal data.

Good reasons why Gaia-X implements SSI

The Internet lacks one essential concept, which has turned out to be necessary for a decentralised and non-monopolised Internet with many concurrent cloud services and nodes, like the Internet Gaia-X intends to establish. This missing part is the identity and trust layer, which is required to consume services and interact with each other in a trustworthy manner.

Today, often we lack options and are stuck using one centralised cloud identity provider with all their pro and cons. However, over the last decades, we witnessed the world becoming increasingly digital and, in conjunction with the mindset changes that involves, a lot of new decentralised Web3 components have emerged that help make the Internet decentralised again – as it was originally designed. One of these concepts is SSI-based on the Web-Of-Trust principle to give back the identity and control of data to the owner.

SSI in a nutshell

A digital identity is a subset of holder attributes that can be used to identify the holder. A holder has several digital identities depending on the context. The subset of attributes of an individual along with the digital identity is called identity data. In a personal authentication case, the username is the digital identity. The password is used to verify the digital identity. The other data such as the full name, address, and details of the payment system are further identity data.
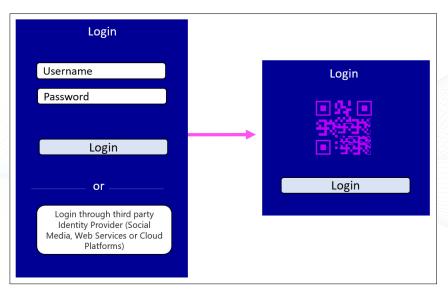

Fig. 1: Login with the present monopolistic identity provider model vs Self-Sovereign and non-monopolistic identity providers.

The reliance on monopolistic identity providers shown in Figure 1 creates a significant dependency for society, companies, and users in the ongoing digitalisation of business and personal fields of life. In addition, the monopolistic identity providers, which are not in Gaia-X, use the sensitive personal data of the users for their own advertising purposes or other economic interests or make them available to other companies. This weakens the privacy of users and has consequences for the acceptance and development of our digital future.

SSI will help, as the sovereignty and protection of the privacy of users are the focus of the new "User-Centric Identity" paradigm and are implemented much better and more user-friendly than in the current "Enterprise-Centric Identity" approach.

Basic structure and process of the SSI ecosystem

With SSI, users control and own their digital identities and other verifiable digital credentials locally. It is not required to use a predominant cloud service provider, nor is the establishment of a central Gaia-X Identity provider necessary. Users are thus completely independent of third parties and decide themselves which identity data they share with whom, as all identity data is securely stored only with the individual user in their SSI wallet.

With SSI, a trustworthy and straightforward peer-to-peer exchange between users and applications does not need a mediator.
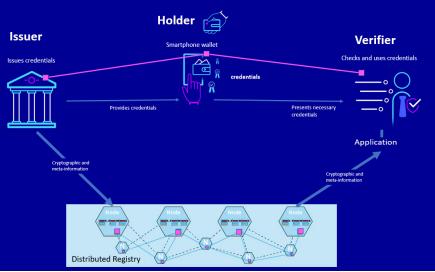

Fig. 2: SSI ecosystem for digital identities and credentials

In the SSI ecosystem for digital identities, an essential role is played by three actors who interact with the SSI infrastructure (principle: trust triangle model), see Figure 2. Each of these actors has a defined task.

Issuer of verifiable credentials

In the SSI ecosystem, *'issuers'* issue verifiable digital credentials, including specific claims (a collection of so-called verifiable credentials), such as certificate claims of identities, confirmations, qualifications, authorisations or membership cards. Samples in the Gaia-X ecosystem are Gaia-X membership credentials, ISO 27001 certifications, BSI C5 attestation, service descriptions, etc., that are referenced and presented in Gaia-X as verifiable self-description presentations (W3C Verifiable Presentation – VP).

Holder (user) of verifiable credentials

SSI denotes a *'holder'* as a user, organisation or technical device which own legitimated verifiable credentials. Usually, the holder securely manages these credentials in their corresponding SSI-capable digital wallet, a so-called SSI wallet agent with selective data discloser functionality.

The wallet agent is not tied to a mobile device. The holder can independently select the best fitting wallet from the comprehensive offerings that are available as integrated browser extensions, as self-hosted or cloud-hosted backend variants and, of course, in the classic form of an app for mobile devices. This enables the respective holder to only share the verifiable digital credential information with the corresponding applications that is indispensable for the initiated process, and no further information is required.

Verification of credential attributes

The *'verifier'* or acceptance points in this SSI ecosystem – e.g. the consumer in the form of an application or a human – require verifiable digital credentials to use and further process the content of the data holder, parts of it or even statements about specific attributes in a process or application (offline or online).

Ideally, this happens fully automatically in a digitised process, which is particularly secure and unambiguous – thanks to the verification of the digital signature. In that verification process, the content and the issuer are clearly cryptographically verified without the need for a direct connection to the issuer.

The architecture of the SSI ecosystem

The advanced Web3 architecture concepts, in contrast to the old cloud architectures, now enable the establishment of a decentralised and self-sovereign ecosystem. This shapes the future of digital identity management in the European Union decisively in a secure, trustworthy and privacy-preserving manner.
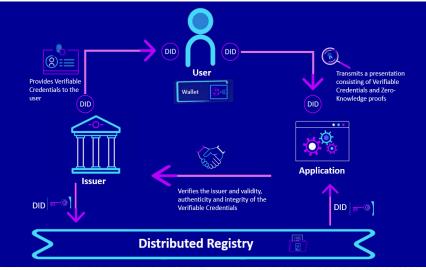

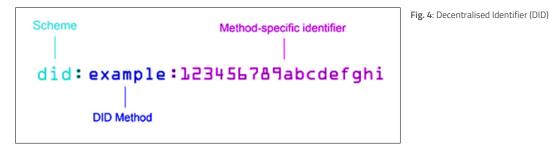**Fig. 3**: Overview of the SSI architecture

The Web3 architecture style helps to support the main self-sovereign principle where users create and manage their digital identities themselves. The whole ecosystem benefits from this decentral architecture concept, which avoids a single point of control as well as a single point of failure in the federated Gaia-X ecosystem.

The architecture goal is to enable interoperability between different SSI solutions. Self-Sovereign Identity uses the W3C specification, Decentralised Identifier (DID), to express unique identifiers for all types of objects and entities. The Verifiable Credentials (VC), on the other hand, for standardised, cryptographically-secured data and identity exchange are based on the well-established JSON (JavaScript Object Notation) format. Optional standards like DIDComm (DIDCommunications) or REST (Representational State Transfer) allow a transport-agnostic communication, usable over HTTPS, WebSockets, BlueTooth, AMQP (Advanced Message Queuing Protocol), SMTP (Simple Mail Transfer Protocol), NFC (Near Field Communication), snail mail, etc. for asynchronous and synchronous message styles.

Decentralised Identifier (DID) Concept

An important characteristic of the SSI concept is the Decentralised identifier (DID). In the SSI ecosystem, DIDs are globally unique and resolvable addresses for entities, individual people, corporations, or digital entities like Gaia-X participants implemented as special W3C Uniform Resource Locators (URLs), like HTTP URLs. The creation and administration of a DID do not depend on a central authority. It is created by the owner themselves with full control over their identifiers and associated key material. In combination with W3C Verifiable Credentials (VC), it gives the owner the ability to de-couple sensitive information from the identifier and make them publicly discoverable for the use of cryptographic proof systems. The owner will selectively use the DID per transaction or generate a new one to prevent correlation.

As with a URL (Uniform Resource Locators), a DID identifies and locates its associated resource, the DID Document. The DID Document is a JSON (JavaScript Object Notation) object in which the associated public keys, lifecycle properties, service endpoints and meta information are included. There is no reference to personal data in the public key. The format of a DID is shown in Fig. 4.

Fig. 4: Decentralised Identifier (DID)

Verifiable Credential (VC) Concept

The Verifiable Credential Data Model defines a standardised data container format for cryptographically signed and verifiable credential data and is also a W3C specification.

The Verifiable Credential Data Model is intended to transfer IT security, trust and privacy, which are valid for physical credentials, to cyberspace through cryptography and supplement them with additional properties and functions.

Fig. 5: Verifiable Credentials

Examples of Verifiable Credentials (see Fig. 6):

- *Certificates of identity* such as personal identity cards. Legal Entity Identification (GLEIF)
- *Certificates* such as ISO 27001 certificates, BSI security certificates, ITIL or TOGAF certificates
- *Attestations*, Gaia-X compliance level, authenticity confirmation, vaccination confirmation
- *Competences* such as a license to practice medicine, data scientist qualification
- *Contracts*, used to specify negotiated cloud service or data usage policies
- *Powers* such as official authority (EU, Gaia-X AISBL) or residence permits
- *Qualifications*, for example, proof of trained personnel to administer cloud services
- *Membership cards*, e.g. Gaia-X membership, club cards, proof of membership of an association or society
- *Loyalty cards* such as bonus cards or frequent flyer programs

These VCs are principally issued to individuals, legal entities, or devices. A VC usually offers the same information content as a comparable physical proof (ID card, membership card).

In contrast to simple data formats like JSON (JavaScript Object Notation), XML (Extensible Markup Language), CSV (Comma-Separated Values file), or even unstructured PDF (Portable Document Format) documents, the W3C-standardised Verifiable Credential data model combines

- the requiring of trust by digital signatures,
- well-formed data structures for digital processing using JSON (JavaScript Object Notation),
- the addition of meaning and semantics to the data structures per linked data schemas with JSON-LD (JavaScript Object Notation Linked Data) standard, and
- proof mechanisms

by applying the Decentralised Identity (DID) concept.

Basically, VCs consist of claims or assertions made about a specific subject, e.g., that a person has a university degree or that a building has a certain height. Furthermore, a VC consists of meta-information that, e.g., specify the type, expiration date or issuer of the VC. With the aim of making the authenticity, integrity, and origin of a VC cryptographically secure and verifiable, the issuers also use the digital signature suite to create a digital signature or a cryptographic proof for a VC.

The proof proves that a VC and its claims about a subject were really created by a specific issuer and was issued to a specific user. Both the subject and the issuer of a VC can be referenced and verified via their respective DIDs. Since the DID of the issuer is contained in the verifiable digital proof, the corresponding DID registry can also be identified with the public key, which is required for the verification, see Figure 6.
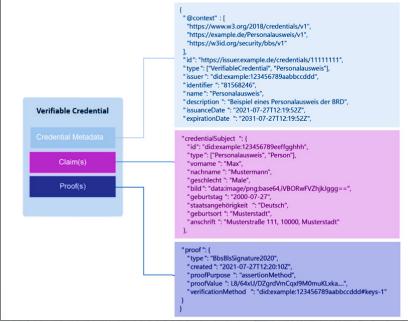

Fig. 6: Example of a Verifiable Credential

Verifiable Credentials are the base of Self-Description

Self-Description (SD) is a major element of the Gaia-X architecture which describes services, participants and data assets. It covers metadata and well-defined claims that consumers can rely on. It uses the trustworthy VC, W3C standards, DID, and associated exchange protocols to define and exchange data with its properties.

Basically, Gaia-X Self-Descriptions can be viewed as verifiable presentations compiled by VCs that express claims or assertions made about a specific subject, e.g., that a participant is a member of Gaia-X or the owner of a certain dataset. Furthermore, the Self-Description data and credentials are managed by the Gaia-X Federation Services (GXFS) component, the Organisational Credential Manager (OCM). It exposes a request interface that the GXFS catalogue and GXFS participants use to collect verifiable information for index building and future service selection processes.

Verifiable Credentials are the base of the Gaia-X Trust Framework and Labelling Concept

As Gaia-X has a higher and unprecedented level of trust for a digital platform, Gaia-X needs to make this trust easy to understand and implementable for all participants. To this end, Gaia-X is developing a Trust Framework and Labelling Framework automating all tests and verifications needed to give a service a specific Label.

Gaia-X will verify the Trust Framework of a service attribute according to those specified for a specific Label/Label level, but will give external authorities (governmental, industry-specific, standardisation bodies, etc.) the ability to define domain-specific Labels. Labels provide a level of assurance without having to examine lengthy and difficult-to-find service credentials.

A single Label can be based on several Trust Framework criteria, of which each one can include one or several Verifiable Credentials. Therefore, Labels make it easy to group criteria and hide the complexity of their verification behind the Gaia-X Trust Framework and Labelling Framework.

The implementation of a Label consists of the decomposition of all Label requirements into Verifiable Credentials that are then encoded in the Gaia-X Trust Framework and Labelling Framework so that they can be verified automatically, where possible. The issuer of a Label can be Gaia-X or another Issuer verified and accepted by the Gaia-X European Association for Data and Cloud AISBL.

Gaia-X Registry

In addition, to ensure a tamper-proof verification scenario, ideally a distributed registry (Distributed Ledger Technology – DLT) can be used as an additional trust layer. DLT is used as a Verifiable Data Registry (VDR) for the secure and trustworthy share of public keys to offer cryptographic protection as an anonymous revocation registry. This concept can be viewed in the long-term as a replacement of a classic Public Key Infrastructure (PKI) with its centralised disadvantages. The Decentralised Identity (DID) concept allows Gaia-X to use different decentralised registries – even standard web domains – to act as a further layer of trust between the actors.
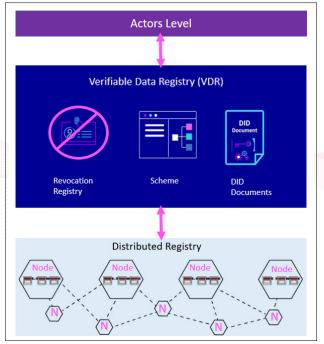

Fig. 7: Distributed Registry as a Verifiable Data Registry

Trustworthy communication

SSI introduced the concept of SSI agents in front of the wallet as a user interface implementing the communication protocols like DIDComm (Decentralised Identity Communication) or OIDC (OpenID Connect) for secure agent-to-agent data exchange. With this separation, the community tries to create a high standardisation of processes and protocols in order to create the highest possible interoperability between different SSI solutions and credential systems.

Therefore, the agent frameworks are used to communicate and exchange Decentralised Identities (DIDs) and Verifiable Credentials (VCs) with one another. Usually, a wallet is also part of an agent, in which the issued VCs can be stored securely. There are different types of agents, but a distinction is usually made between mobile and cloud or institutional agents. While mobile agents can be present on the smartphone in the form of applications, cloud agents are applications or services that are operated on a server, see Figure 8.
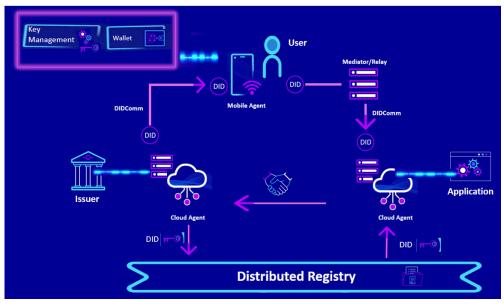

Fig. 8: Conceptual image of SSI Agents and DIDComm

The standardisation efforts of the Hyperledger Aries Project, Decentralized Identity Foundation (DIF) and W3C (World Wide Web Consortium) not only enable interoperability on the client layer but also reflect on the underlying registry level. The past dependency on Hyperledger Indy as a blockchain-based registry for SSI Frameworks continues to decrease. This has led to the choice of registry in the form of Distributed Ledger Technology (DLT) by the providers of SSI becoming more flexible.

Use of SSI in Gaia-X Federation Services

In traditional, centralised cloud ecosystems, identities and associated credentials like accounts, Gaia-X membership, attestations, or ISO (International Organization for Standardization) certification documents, etc., required for operations are hard to exchange in a trustworthy and privacy-preserving way.

If Gaia-X were not to use SSI, it would perpetuate the system of centralised identity and trust providers that we currently use on a day-to-day basis. There are advantages to this system, as well as disadvantages. Not knowing how good the privacy of these central identity providers is and to what extent they are protected from misuse is a reason why Gaia-X participants should not use them. No participant should lose the control and sovereignty of their data or give a provider the possibility to monitor and restrict them in the future in some critical situations. Hence a Gaia-X key differentiator is the ability to establish a fully decentralised and autonomously managed ecosystem anchored in the Gaia-X Federation Services (GXFS) Identity and Trust concept, whereby each actor can interact with any other participant in a direct way. In addition to decentral Identity Management & Trust, GXFS will utilise SSI in different areas:
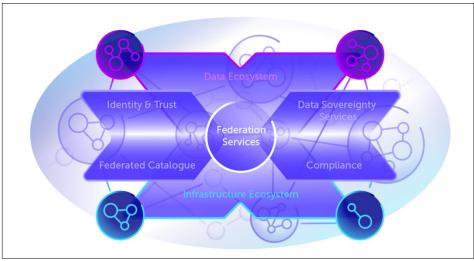
Fig. 9: Gaia-X Ecosystem

Identity & Trust:
- Self-Issued OpenIDProvider (SIOP) for decentral authentication
- Attribute-based authorisation with credentials over role-based access control
- Self-management of credentials through secure wallets for persons and organisations
- Software agent for selective self-discloser with signed and verifiable credentials and Self Descriptions
- Providing technical trust methods and trust anchor interfaces

Federated Catalogue:
- Providing trustworthy data for search index generation through cryptographical verifiable Self Descriptions and associated attestations
- Trustworthy interlinking of service offerings and service provider
- Protection of Self Description attributes with selective data disclosure functionality

Compliance:
- Notarisation functionality to transform paper certificates and attestation into corresponding digital verifiable credentials
- Issue digital and verifiable membership credentials with eIDAS conform signatures
- Manage compliant trust and revocation lists for digital verification
- Fraud control

Data Sovereignty Services:
- Deliver the base of capability-based access control through credentials
- Enhance data privacy and protection through zero-knowledge proof, including selective disclosure capabilities
- Ensure the authenticity of the data owner, provider and consumer in a digitally verifiable manner
- Creation of digital incontestable data sharing contracts
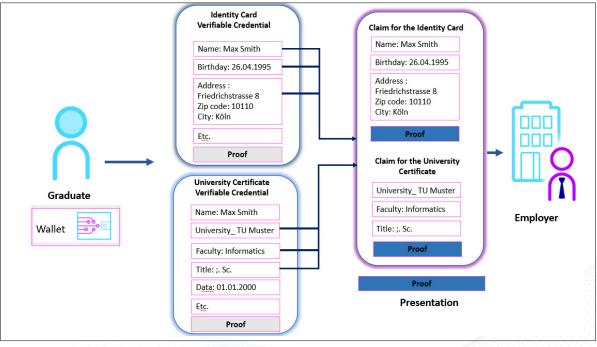- Establishing trusted and secured data sharing connections

Portal:
- Authentication and access control with bridge functionality to connect to an existing OpenID Connect IAM (Identity and access management) infrastructure

SSI in the Context of Data Exchange and Data Protection

As well as data encryption, the application of SSI zero-knowledge proof concepts and Attribute-Based Access Control (ABAC) enables future zero-trust and privacy protection architectures, without the disadvantages of static Role-Based Access control (RBAC). Among other things, Zero-Knowledge Proofs (ZKP) are essential cryptographic functions that allow data protection-compliant and data-saving exchange of Verifiable Credentials (VCs) in the context of SSI. With these special digital signature suites, VCs are cryptographically signed by the issuer in a special way when they are created to be able to implement the following ZKP mechanisms.

Selective Disclosure

If a user wishes to use their VCs as digital proof in an application, the application would be presented with the required VCs in their entirety in a presentation for verification without the use of ZKPs. As a result, applications may receive significantly more information or claims about a user than are actually needed for the intended use case. Selective disclosure can be used to make the information transfer more fine-grained and reduce it to the absolute minimum. With this function, it is possible to disclose only certain claims from one or more VCs in a secure and trustworthy manner and to prove them cryptographically, see Fig. 10.

Fig. 10: Targeted information transfer through Selective Disclosure

Through selective disclosure, information within a used VC that is not requested or required by the application can be hidden during the presentation. When issuing a VC, the issuer uses a special multi-message signature suite to individually sign each claim within the VC. Instead of just the VC, a subset of the claims of a VC can be presented without the digital signature losing its validity. It is also possible to use certain claims from different VCs for a presentation.

An example of selective disclosure would be if a user wants to share or provide proof of their address to an application. The user can, e.g., use VCs of their identity card, consisting of the claims name, date of birth, address, height etc. and only release the claims name and address for the application. All claims of the application that are not required remain hidden (date of birth, height, etc.). This example clearly highlights the difference between a Verifiable Credential and a physical credential like a passport. While functions such as selective disclosure can be used with a verifiable credential, no information can be selectively hidden when using a physical credential for verification or authentification.

Predicate Proofs

Predicate proofs are another essential component of Zero-Knowledge Proofs (ZKP) and often help to implement the General Data Protection Regulation (GDPR) and confirm privacy and data protection aspects simply and effectively, as information can be cryptographically verified without having to disclose the information values to a requester. Because instead of disclosing information, cryptographic material is used to provide calculated predicate proofs, such as "greater than 18", "less than 18", or "equal to".

There are use cases in which it is necessary, for example, to check whether a person is solvent, a predicate proof presents only the cryptographical statement that the account in question is covered up to €10,000, instead of sharing the exact account balance.

Signature Blinding

A presentation that is transmitted by the user to an application contains a number of verifiable credentials that have been digitally signed by the respective issuer. With the help of the digital signature, the authenticity and integrity can be verified, and it is therefore of elementary importance for the SSI ecosystem. In spite of all of this, signatures offer a potential target for correlations because digital signatures are unique identifiers and are consequently a factor that can be correlated.

Signature blindings are used to avoid a potential correlation of the digital signatures. Signature blinding can be used to cryptographically hide the digital signature or the corresponding proof of an issuer by randomising the digital signature before it is passed on to an application. During this process, the validity and origin of Verifiable Credentials (VCs) and presentations remain verifiable.

Private Holder Binding

With the private holder binding, it is possible to bind a VC cryptographically to a user and to prove this connection later without using or disclosing the user's Decentralised Identity (DID). For this purpose, individual link secrets are used to which VCs can be cryptographically linked. The advantage, through the indirect connection of the VC to the user, is that the DID is no longer required as a clear correlation factor and thus represents a cryptographic and data protection-friendly alternative.

Conclusion

In the Gaia-X ecosystem, the use of open W3C (World Wide Web Consortium) specifications such as the Decentralised Identifier (DID) and the Verifiable Credential (VC) data model as well as open-source projects such Hyperledger Aries, ESSIF (European Self-Sovereign Identity Framework) or IDUnion promotes the continuous further development of Self-Sovereign Identity (SSI). It also enables interoperability between SSI solutions and other credential systems. The usage of Web3 concepts and decentralised technologies enables Gaia-X members to build their own autonomous Gaia-X Federations without the need of a central controlling Gaia-X instance.

Distributed ledgers in combination with the Self-Sovereign Identity ecosystem is not mandated, however, they can be integrated to generate additional trust, flexibility and scalability. Agents for managing the digital identity and usage of advanced SSI-standard communication protocols are sensible concepts that allow data privacy in a user-friendly application of DIDs and Zero-Knowledge Proofs (ZKP)-enabled VCs – without overwhelming the user with their complexity and administrative effort. The SSI ecosystem removes the dependency on individual market leaders and gives users the freedom to shape the digital future more independently and more successfully. As a digitalisation accelerator, SSI ensures faster, more secure, and more trustworthy digitalisation. With SSI, the users in the Gaia-X ecosystem are enabled to choose selectively both the level of privacy and to which party they transmit all or a selected subset of their identity and associated data to the cloud applications. This creates a high degree of privacy, value-oriented IT and services, and thus a high level of acceptance for the digital future.
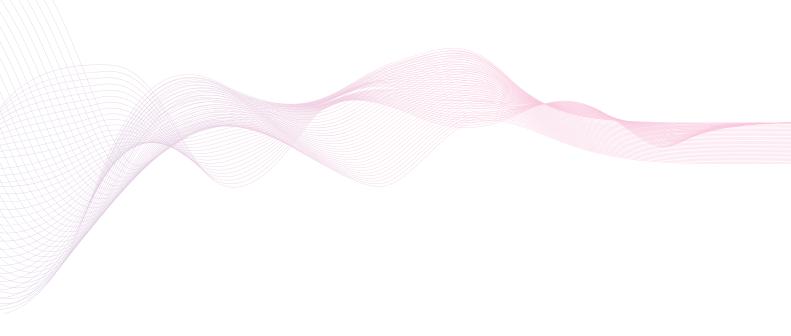
Authors:

Berthold Maier (Telekom - T-Systems International) Chief Architect and SSI expert

Berthold Maier has worked as Head of Architecture in the Industry, Telecommunication and Public Sector sectors for over two decades. He is the Chief Architect at T-Systems for the German Federal Office for Migration and Refugees (BAMF) and is the Lead for the GAIA-X Federated Services (GXFS) Identity and Trust. Prior to that, he was the CTO of Digital Solutions within T-Systems.

Prof. Dr. Norbert Pohlmann (eco) Board member responsible for IT security

Norbert Pohlmann is a Professor of Computer Science in the field of cybersecurity and is Head of the Institute for Internet Security - if(is) at the Westphalian University of Applied Sciences in Gelsenkirchen, Germany, as well as Chairman of the Board of the German IT Security Association TeleTrusT, and a member of the board at eco – Association of the Internet Industry.

Association Name: Gaia-X European Association for Data and Cloud AISBL
Contact Person: Dr. Vassilia Orfanou, CMO
Phone: +306974825327
Email: vassilia.orfanou@gaia-x.eu
Address: Avenue des Arts 6-9, 1210 Brussels, Belgium
Website: www.gaia-x.eu

Company Name: eco – Association of the Internet Industry
Contact Person: Mareike Zeisig, Marketing Manager
Phone: +49 (0) 221 - 70 00 48 - 107
Email: mareike.zeisig@eco.de
Address: Lichtstr. 43h, 50825 Köln, Germany
Website: www.gxfs.eu